Improvements in Transportation Security Analysis from a Complex Risk Mitigation Framework for the Security of International Spent Nuclear Fuel Transportation

Adam D. Williams
Global Security Research & Analysis
Sandia National Laboratories
Outline

- Introduction

- Risk Complexity & International SNF Transportation
  - A New Conceptual Approach for Risk Complexity
  - Novel Analysis Tools for Risk Complexity

- Lessons from Learned from Risk Complexity in International SNF Transportation

- Implications for Transportation Security

- Summary & Conclusions
Introduction

- The nuclear fuel cycle faces **more complex risks** from a growing & evolving operational environment
  - Interdependencies between security, safety & safeguards (3S) risks & dynamic operational environments challenge traditional risk analysis methods

- Exemplified in the multi-modal or **multi-jurisdictional complexity** of the international transport of spent nuclear fuel (SNF)
  - 1996 shipment of HEU from Colombia to U.S.
  - Agreed shipment of SNF from Iran to Russia
Introduction

According to Olli Heinonen (2017):

- ‘Safeguards, security, and safety’ are commonly seen as separate areas in nuclear governance. While there are technical and legal reasons to justify this, they also co-exist and are mutually reinforcing. Each has a synergetic effect on the other…’

Recently completed LDRD research at Sandia National Laboratories explored integrated safety, security & safeguards (3S) frameworks for managing risk complexity in international SNF transportation

- The results of this study present intriguing implications reducing transportation security risk(s) against 21st century threats
Risk Complexity

- A new concept of risk that, for international SNF transportation, that includes
  - The traditional definitions of risk associated with security, safety & safeguards
  - Social and political contexts/dynamics that may prevent the completion of the desired safety, security and safeguards objectives
  - The emergence of risk resulting from interactions among security, safety, and safeguards risks and mitigations
Risk Complexity

- Incorporating complexity & systems theories into traditional engineering approaches to risk introduces:
  - **Interdependence**: how interactions influence desired functions
  - **Emergence**: how system level behavior results from interactions
  - **Hierarchy**: how higher levels constrain the behaviors of lower levels

- The result: a state-space description of complex risk where
  - \((T)\) = total state space
  - \((D)\) = some subset of \((T)\) representing all desirable system states
  - \((T-D)\) = a complementary subset representing the undesirable, or ‘risky,’ states

- All else equal, complex risk is manipulating the technical/social components of a system to stay in the desirable system states
Risk Complexity

- Such systems may exist at **different places** in the desirable space at **different points in time**
  - Complex risk is dynamic and also includes all system states between beginning & end points
  - The requirements that define the desirable space are implemented in different social, political, and technical contexts.

- Therefore, while Figure (a) may appear to have relatively low risk at Nodes A and B, Figure (b) illustrates how there are multiples points that approach the boundary of the desirable space.
**Risk Complexity**

**Dynamic Probabilistic Risk Assessment (DPRA)**
- Bottom-up & deterministic
- Uses Dynamic Event Trees (DETs) for systematic and automated assessment of possible scenarios arising from uncertainties
- Models/tools used:
  - Safety: RADTRAN
  - Security: STAGE
  - Safeguards: PRCALC, Markov Chain model of safeguards from BNL

**System-Theoretic Process Analysis (STPA)**
- Top-down & based on system-level behaviors
- Based on abstracting real complex system operations into hierarchical control structures & functional control loops
- Two Primary Steps:
  - ‘Step One’: identify possible violations of control actions that lead to system states of higher risk
  - ‘Step Two’: derive specific scenarios that could cause these theorized violations to occur

---

Courtesy: Leveson 2012

Courtesy: Kalinina, et. al. 2017
Lessons from SNF Transportation

- **Improved** understanding over traditional approaches to transportation security risk
- **Enhanced** understanding & ability to manage increasing risk complexity
- **Distinguishing** sources of risk that can be controlled (i.e., defining & high level requirements) from those that cannot (i.e., inherent risk of shipping)
- **Identifying** sources of risk variability (e.g., those from implementation vs. those regardless of implementation)

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Traditional Characterization (e.g., security in isolation)</th>
<th>Complex Risk Characterization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Definition</td>
<td>Probabilistic ability to protect along path(s) against anticipated adversary capabilities</td>
<td>Emerges from potential system migration toward states of higher risk</td>
</tr>
<tr>
<td>Risk Reduction</td>
<td>From improved component reliability &amp; defense-in-depth</td>
<td>Realized as part of complex risk management trade-space</td>
</tr>
<tr>
<td>Risk Measure</td>
<td>System effectiveness (e.g., combinatorial reliability of security components)</td>
<td>State description including nuclear material loss, area contamination &amp; socioeconomic harms</td>
</tr>
<tr>
<td>Solution Space</td>
<td>Limited to increasing security component reliability or reducing adversaries capabilities</td>
<td>Expanded to technical, organizational or geopolitical influences &amp; safety/safeguards leverage points</td>
</tr>
<tr>
<td>Relationship to Safety &amp; Safeguards</td>
<td>None, treated as an independent risk</td>
<td>Parallel characteristic, treated as interdependent component of complex risk</td>
</tr>
</tbody>
</table>
Lessons from SNF Transportation

- A potential **paradigm shift** in risk assessment & management for international SNF transportation security (and, nuclear fuel cycle activities writ large)
  - Risk from the ‘inside out’ as a dynamic balance within a system state-based tradespace

- Additional major lessons include:
  - realities of international SNF transportation will challenge current approaches and assumptions;
  - risk itself is complex;
  - some aspects of/influences on risk are controllable, some are not;
  - 3S interdependencies exist;
  - risk is a complex trade space; and,
  - integrated 3S risk management frameworks can reduce risk/uncertainty, even for individual (e.g., security only) perspectives
These conclusions offer a better understanding of 3S interactions that can improve SNF transportation security design & analysis.

<table>
<thead>
<tr>
<th>Lessons Learned</th>
<th>Implications for SNF Transportation Security</th>
</tr>
</thead>
</table>
| Realities of international SNF transportation will challenge current approaches and assumptions | • Need to (re)assess the validity of assumptions underlying current approaches to transportation security  
• Technical analysis tools need to account for the variation in implementation of the PPS in transit among different operators |
| Risk itself is complex                                                         | • Security risk metrics (e.g., system effectiveness, $P_E$) may be insufficient to adequately describe security risk/assess vulnerabilities  
• Need to identify key aspects/descriptors of new challenges to transportation security |
| Some aspects of/influences on risk are controllable, some are not               | • Not all security risks lie in adversary action or can be described in probabilistic/technical reliability terms  
• Implementation decisions & how technical components within transportation security systems matter—and should be included in analytical frameworks |
Implications for Transportation Security (2/2)

- These conclusions offer a better understanding of 3S interactions that can improve SNF transportation security design & analysis

<table>
<thead>
<tr>
<th>Lessons Learned</th>
<th>Implications for SNF Transportation Security</th>
</tr>
</thead>
</table>
| **3S interdependencies exist** | • Need to change the assumption that transportation security can be accurately & adequately evaluated independently  
• A broader solution space exists for managing complex risk in transportation security (e.g., leveraging safeguards material accounting practices to mitigate insider issues) |
| **Risk is a complex trade space** | • There is no ‘true’ minimization of security risk, therefore attempts at security design optimization are more complex  
• Need to develop expertise/experience in making security-related trade-offs during international SNF transportation |
| **Integrated 3S risk management frameworks can reduce risk/uncertainty, even for individual perspectives** | • Integrated approaches have been shown to incorporate more contributor to complex risk  
• Need to develop new analytical approaches to assess non-uniform, larger types of uncertainty (between safety, security & safeguards) |
Conclusions

- This SNL study demonstrated how incorporating complexity & systems theories supports \textit{complex risk}, a concept that better addresses
  - Non-traditional risk-related pressures & dynamics (e.g., social contexts & changing security implementation capabilities)

- Related insights offer improved management strategies to ensure the protection of nuclear (& radiological) materials against dynamic, complex risks while in transit

- This concept provides implications for improving SNF transportation security—and security of nuclear materials in transit more generically—against 21st century threats